IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:	)
	)
Kelly et al.	) Art Unit: 2131
	)
Application No. 10/028,906	) Examiner: LAFORGIA, CHRISTIAN A.
	)
Filed: 12/28/2001	) Atty. Docket No.:
	) NAI1P484/01.103.01
For: CONTROLLING ACCESS TO SUSPICIOUS	)
FILES	) Date: January 15, 2007
	)
	)

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

ATTENTION: Board of Patent Appeals and Interferences

REPLY BRIEF (37 C.F.R. § 41.37)

This Reply Brief is being filed within two (2) months of the mailing of the Examiner's Answer mailed on 11/13/2006.

Following is an issue-by-issue reply to the Examiner's Answer.

The Examiner has rejected Claims 1-13 and 27-39 under 35 U.S.C. 101 as being directed toward non-statutory subject matter.

     Group #1: Claims 1-13

The Examiner has rejected Claims 1-13 under 35 U.S.C. 101 as being non-statutory, since such claims allegedly represent a computer listing *per se*, that is, non-functional descriptive material, etc. Appellant respectfully disagrees. Specifically, appellant clearly claims a "computer program product for <u>operating a computer to review files for potential malware</u>" (emphasis added), clearly a functional set of acts being performed.

In the Examiner's Answer mailed 11/13/2006, the Examiner argues that 'the recitation "operating a computer to review files for potential malware" has not been given patentable weight because the recitation occurs in the preamble.' Appellant respectfully disagrees and asserts that the claimed "computer program product for operating a computer to review files for potential malware, compris[es]: logging code…weighting table code…statistical log interface code…[etc.]" which all perform functional operations when executed, as claimed.

Also in the Examiner's Answer mailed 11/13/2006, the Examiner argues that '[t]he plain meaning of the term "operable" as understood by the Examiner means "capable of being put into use, operation or practice"' and that "Appellant never states that the code is running or executing, but merely that there is a possibility that the code or logic may be executed." Additionally, the Examiner "interprets the limitations of claims 1-13… as representing a computer listing *per se* that is capable of being executed, but never actually implemented."

Appellant respectfully disagrees and again notes that appellant clearly claims a "computer program product for <u>operating a computer to review files for potential malware</u>" (emphasis added), as claimed.

     Group #2: Claims 27-39

The Examiner has rejected Claims 27-39 under 35 U.S.C. 101 as being non-statutory, since such claims allegedly represent a computer listing *per se*, that is, non-functional descriptive material, etc. In the Examiner's Answer mailed 11/13/2006, the Examiner "interprets the limitations of claims... 27-39 as representing a computer listing *per se* that is capable of being executed, but never actually implemented." Appellant respectfully disagrees. Specifically, appellant clearly claims a "data processing apparatus for reviewing files for potential malware comprising: logging logic...weighting table logic...[etc.]" (emphasis added), as claimed.

Issue # 2:

The Examiner has rejected Claims 1-2, 7-12, 14-15, 20-25, 27-28, and 33-38 under 35 U.S.C. 103(a) as being unpatentable over Chess et al. (U.S. Patent No. 6,711,583), in view of Smithson et al. (U.S. Patent No. 6,886,099).

   Group #1: Claims 1-2, 7-10, 12, 14-15, 20-23, 25, 27-28, and 33-36, 38

With respect to each of the independent claims, the Examiner has responded to appellant's arguments with respect to appellant's claimed "logging code operable to maintain a statistical log having an entry for each file sent to the computer for review, each entry being arranged to store a count value indicating the number of times that the file has been sent to the computer for review and a value of one or more predetermined attributes relating to the file" (see this or similar, but not necessarily identical language in each of the independent claims).

Specifically, the Examiner has stated that the Abstract of Smithson teaches "the tracking for a number of times a file is sent for review." Appellant respectfully asserts that the Abstract in Smithson only discloses measuring "how many E-mail messages are sent having an identical file attachment, the file type or simply in total." Clearly, measuring how many E-mail messages are sent, as in Smithson, does not meet appellant's specific claim language, namely "stor[ing] a count value indicating the number of times that the file has been sent to the computer for review" (emphasis added), as claimed.

In addition, the Examiner has stated that Col. 5, lines 5-48 in Chess teach "keeping a value of one or more predetermined attributes relating to the file, such as whether the file is safe or questionable." First, appellant respectfully asserts that such excerpt in Chess only teaches "examin[ing] documents in the collection on disk," and not "a statistical log having an entry for each file sent to the computer <u>for review</u>," as appellant claims (emphasis added). Second, Chess merely discloses storing "the document name and macro data" associated with the document, where the macro data is the <u>names</u> of any macro data stored in the document. Clearly, such data does not meet appellant's claimed "<u>value</u> of one or more predetermined attributes relating the file" (emphasis added). Thus, in view of the above arguments, appellant respectfully asserts that neither Smithson nor Chess meet appellant's specific claim language.

In the Examiner's Answer mailed 11/13/2006, the Examiner has argued that "*Chess* discloses… a database of document information (Figure 2 [block 204], column 4, lines 22-61) that maintains an entry for every file on the computer" and that "*Chess* further goes on to state that the database can maintain a number of times the document has been reviewed for changes (column 4, line 62 to column 5, line 5)."

Appellant disagrees and respectfully notes that the excerpts from Chess relied on by the Examiner merely teach that "the database 204 contains, for each document in the collection, the name of the document and data pertaining to any program objects such as macros, programs or other units of active content… contained in the document" (Col. 4, lines 30-34). The excerpts further teach that a "scan [of the system] can be initiated in response to a document changing event such as each occurrence of a document changing" (Col. 4, line 67 – Col. 5, line 2). However, merely disclosing the existence of a <u>document information database</u> as well as <u>system scanning</u> in response to a document changing event, as in Chess, does not teach "logging code operable to maintain a <u>statistical log</u> having an entry for each file <u>sent to the computer for review</u>, each entry being arranged to store a count value indicating the <u>number of times</u> that the file has been sent to the computer <u>for review</u> and a value of one or more predetermined attributes relating to the file" (emphasis added), as claimed by appellant. Clearly, initiating a scan in response to a document <u>changing</u> event, as in Chess, simply fails to even suggest "each entry being arranged to store a count value indicating the <u>number of times</u> that the file has been sent to the computer <u>for review</u>" (emphasis added), in the manner as claimed by appellant.

Still with respect to each of the independent claims, the Examiner has responded to appellant's claimed "weighting indicating the likelihood that a file having that value of said one or more predetermined attributes will be malware" and "referenc[ing] the weighting table to determine the weighting to be associated with the file, based on the value of said one or more predetermined attributes associated with that file in the statistical log" (see this or similar, but not necessarily identical language in each of the independent claims).

Specifically, the Examiner has argued that "Chess discloses a technique for determining the likelihood of a file being infected by the addition or change of code since the last time the file has been reviewed" (Col. 5, lines 5-48). Appellant respectfully asserts that simply comparing macro data to determine if "safe" changes or "questionable" changes have occurred, as in Chess, does not even suggest any sort of <u>weighting table</u>. Instead, Chess teaches that "removing one or more macros from the document could be considered 'safe', whereas the modification or addition of macros to the document could be considered 'questionable'."

Thus, Chess determines whether a document has safe or questionable changes made to it based on whether a change involved the removal or addition of macros, which clearly does not even suggest the utilization of a weighting table, and especially not in the context claimed by appellant. In addition, since Chess does not disclose storing any sort of <u>value</u> of one or more predetermined attributes relating to the file, in the manner claimed by appellant, Chess simply would not utilize a <u>weighting</u> table for determining the weighting to be associated with the file, based on the <u>value</u> of said one or more predetermined attributes associated with that file, as appellant specifically claims.

In the Examiner's Answer mailed 11/13/2006, the Examiner has argued that "*Smithson* teaches various parameters are measured and compared to threshold levels, and if the parameters exceed the threshold levels set forth than that file contains malware, see, for example, column 4, lines 5-20" and that therefore "*Smithson* discloses a weighting table to determine a weighting associated with the file…in the discussion of exceeding various measurement parameters and exceeding certain thresholds." The Examiner has further argued that "*Chess* discloses determining the

likelihood of a document being infected with a virus based on data stored in the document information database, as seen in… column 4, line 62 to column 5, line 5."

Appellant disagrees and respectfully points out that the excerpts from Smithson relied on by the Examiner merely teach "<u>monitoring</u> one or more <u>measurement parameters</u> obtained over a measurement period against predetermined threshold levels" (Col. 4, lines 6-8 – emphasis added). In addition, the parameters measured only relate to the "<u>activity of the computer system as a whole</u> over a measurement period" (Col. 2, lines 3-4 – emphasis added) and "can include a measurement of how many E-mail messages are sent having an identical file attachment, file type or simply in total" (Abstract – emphasis added). However, merely <u>monitoring</u> the "<u>activity of the computer system as a whole</u>" against threshold levels, as in Smithson, fails to teach "<u>weighting</u> indicating the likelihood that a <u>file</u> having that value of said one or more predetermined <u>attributes</u> will be malware" (emphasis added), as claimed by appellant. Clearly, monitoring one or more measurement parameters over a period, as in Smithson, fails to suggest a "<u>file</u> having that value of said one or more predetermined <u>attributes</u>" (emphasis added), in the manner as claimed by appellant.

Additionally, appellant again respectfully notes that the excerpt from Chess relied on by the Examiner merely discloses the existence of a <u>document information database</u> that stores "data pertaining to any program objects…contained in the document" (Col. 4, lines 30-34), as well as <u>system scanning</u> in response to a document <u>changing</u> event, which in no way teaches "referenc[ing] the <u>weighting table</u> to determine the <u>weighting</u> to be associated with the <u>file</u>, based on the value of said one or more predetermined attributes associated with that file in the statistical log" (emphasis added), as claimed by appellant. Appellant respectfully asserts that the data stored in the database disclosed in Chess only includes a number of macros, a total length of macros, a length of each macro, a checksum of each macro, etc. (see Col. 4, lines 34-61). However, nowhere in the excerpts relied on by the Examiner is there any suggestion of "<u>weighting</u> indicating the likelihood that a file having that <u>value</u> of said one or more <u>predetermined attributes</u> will be malware" (emphasis added), as claimed. In addition, a document <u>changing</u> event, as in Chess, fails to suggest "referenc[ing] the <u>weighting table</u> to determine the <u>weighting</u> to be associated with the <u>file</u>" (emphasis added), in the manner as claimed by appellant.

-6-

Still with respect to each of the independent claims, the Examiner has failed to respond to appellant's arguments with respect to appellant's claimed "statistical log interface code operable, upon receipt of a file, to determine with reference to the statistical log the count value relating to that file; action determination code operable, if the count value determined by the statistical log interface code exceeds a predetermined threshold" (see this or similar, but not necessarily identical language in each of the independent claims). In particular, the Examiner has merely stated that "the combination of [Smithson and Chess] disclose referencing a weighting table to determine the weighting to be associated with the file, based on the value of said one or more predetermined attributes associated with that file in the statistical log."

Appellant respectfully asserts that what is claimed is "determin[ing] with reference to the statistical log <u>the count value</u> relating to that file" (emphasis added). For substantially the reasons argued above, appellant emphasizes that neither Chess nor Smithson teach any sort of <u>value</u> in the context claimed by appellant, and thus it is impossible for the references to teach a situation where "upon receipt of a file...determin[ing] with reference to the statistical log the count value relating to that file," as claimed by appellant.

In the Examiner's Answer mailed 11/13/2006, the Examiner has argued that "at column 5, lines 11-16, *Chess* states that the document database disclosed above is consulted for each document, thereby providing for sometime of interface for the database" and that "*Chess* discloses maintaining a count value in the database."

Appellant disagrees and respectfully notes that the above excerpt from Chess relied on by the Examiner simply teaches that "the module... consults the database 204 to determine the previous state of the document [in the collection]" (Col. 5, lines 13-16) and that that "the database... contains, for each document in the collection, the <u>name</u> of the document and <u>data pertaining to any program objects</u> such as macros, programs or other units of active content... contained in the document" (Col. 4, lines 30-34). However, consulting a database to determine the state of a document, in addition to storing the <u>name</u> of a document and <u>program object data</u> in a database, as in Chess, fails to disclose "statistical log interface code operable, upon receipt of a file, to determine with reference to the statistical log the <u>count value</u> relating to that file" and "action

determination code operable… if the <u>count value</u> determined by the statistical log interface code exceeds a predetermined threshold," where "a <u>count value</u> indicat[es] the number of times that the file has been <u>sent to the computer for review</u>" (emphasis added), in the context as claimed by appellant.

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on appellant's disclosure. *In re Vaeck,* 947 F.2d 488, 20 USPQ2d 1438 (Fed.Cir.1991).

In the Examiner's Answer mailed 11/13/2006, the Examiner has argued, with respect to the first element of the prima facie case of obviousness of combining the aforementioned references, that "*Smithson* provides for motivation to combine the references at column 2, lines 10-15 stating that the combination provides for a method to detect unknown viruses more readily, thereby preventing infection of computer systems." To the contrary, appellant respectfully asserts that it would not have been obvious to combine the teachings of the Chess and Smithson references, especially in view of the vast evidence to the contrary.

Specifically, Smithson *teaches away* from Chess's technique of detecting document-infecting viruses by disclosing that "the technique of the invention is … able to more readily detect previously unknown viruses by the effect that they have on the activity of the <u>computer system as a whole</u>" (Smithson, Col. 2, lines 11-15 – emphasis added). Clearly, Smithson is concerned with the activity of the computer system as a whole, where Chess is concerned with the changes in individual documents infected by viruses. It is improper to combine references where the references teach away from their combination. *In re Grasselli*, 713 F.2d 731, 743, 218 USPQ 769, 779 (Fed. Cir. 1983). To this end, the Examiner's proposed combination is clearly inappropriate.

Appellant respectfully asserts that at least the first and third elements of the *prima facie* case of obviousness have not been met, since it would not have been obvious to combine the prior art references, and since the prior art references, when combined, fail to teach or suggest <u>all</u> of the claim limitations, as noted above.

   Group #2: Claims 11, 24, and 37

Appellant again notes that the Examiner has relied on the following excerpts from the Smithson reference to make a prior art showing of appellant's claimed "each entry in the statistical log … further arranged to identify, for each sender of that file, the number of times that that sender has sent the file in addition to the count value indicating the total number of times that the file has been sent" (see this or similar, but not necessarily identical language in each of the independent claims).

```
"As preferred examples of the measurement parameters that may be used
there are proposed:
1. How many E-mail messages are sent having an identical message title.
2. How many E-mail messages are sent identical file attachment.
3. How many email messages are sent having a file attachment of a given
file type.
4. How many E-mail messages are sent having a file attachment that is
an executable file.
5. The E-mail through put within the computer system.
6. The E-mail throughput measured in a form dependent upon a number of
E-mails multiplied by a total size for the E-mails."
(Col. 4, lines 25-40)
```

Again, as noted above, Smithson's measurement parameters and thresholds are associated with aggregate file <u>activity</u>, and not a particular file. To this end, Smithson simply fails to meet appellant's claimed "number of times that that sender has sent the file in addition to the count value indicating the total number of times that the file has been sent," as claimed. It is further noted that the measurement parameters does not track a per-sender number, and thus fails to meet appellant's claimed "each entry in the statistical log … further arranged to identify, <u>for each sender of that file</u>, the number of times that that sender has sent <u>the file</u> in addition to the count value indicating the total number of times that the file has been sent" (emphasis added), as claimed by appellant.

Thus, only appellant teaches and claims use of both 1) a number of times that a <u>particular</u> sender has sent a file, <u>and</u> 2) a <u>total</u> number of times the file has been sent *irrespective of sender* in each entry in the statistical log. Note Table 1 below which illustrates such claimed subject matter.

<u>Table 1</u>

Entry_1 (associated with file_1)

      Sender_1
            Number of times file_1 is sent by Sender_1
      Sender_2
            Number of times file_1 is sent by Sender_2
      Total number of times file_1 is sent

Entry_2 (associated with file_2)

      Sender_1
            Number of times file_2 is sent by Sender_1
      Sender_2
            Number of times file_2 is sent by Sender_2
      Total number of times file_2 is sent

In the Examiner's Answer mailed 11/13/2006, the Examiner "agrees that *Smithson* does not explicitly state a number of times a sender transmits a file" but has argued that "*Smithson* provides examples of various measurement parameters that can be arranged by a system manager." Additionally, the Examiner has simply dismissed dependent Claim 11 et al. under Official Notice. Specifically, the Examiner has argued that "[a]s admitted by the Appellant, *Smithson* teaches wherein a number of times a file is sent is tracked" and that "[o]ne of ordinary skill in the art would recognize that it would be simple to modify the example rules outlined in *Smithson* to track the number of times a particular sender transmits the same file."

Appellant respectfully disagrees. In particular, appellant respectfully asserts that appellant has <u>not</u> admitted that *Smithson* teaches wherein a <u>number of times a file is sent</u> is tracked, as the

Examiner notes. Appellant respectfully points out that, as mentioned previously, Smithson discloses "suitable measurement parameters" (Col. 4, lines 24-25), and further teaches that the parameters measured relate to the "activity of the computer system as a whole over a measurement period" (Col. 2, lines 3-4 – emphasis added). However, merely disclosing measurement parameters and thresholds that are associated with aggregate file activity, as in Smithson, does not even suggest a technique where "each entry in the statistical log is further arranged to identify, for each sender of that file, the number of times that that sender has sent the file in addition to the count value indicating the total number of times that the file has been sent" (emphasis added), as claimed by appellant. Clearly, measurement parameters and thresholds for aggregate file activity across a computer system, as in Smithson, fails to specifically suggest "the number of times that that sender has sent the file in addition to the count value indicating the total number of times that the file has been sent" (emphasis added), in the manner as claimed by appellant.

Thus, appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above.

Since the Examiner has not established all of appellant's claim limitations in the prior art, it appears that the Examiner has relied on an inherency argument regarding the above emphasized claim limitations. The fact that a certain result or characteristic may occur or be present in the prior art is not sufficient to establish the inherency of that result or characteristic. *In re Rijckaert*, 9 F.3d 1531, 1534, 28 USPQ2d 1955, 1957 (Fed. Cir. 1993); *In re Oelrich*, 666 F.2d 578, 581-82, 212 USPQ 323, 326 (CCPA 1981). Rather, to establish inherency, the extrinsic evidence must make clear that the missing descriptive matter is necessarily present in the thing described in the reference, and that it would be so recognized by persons of ordinary skill. Clearly, the above emphasized limitations are not *necessarily present* in *Smithson*, as even admitted by the Examiner. In view of the arguments made hereinabove, any such inherency argument has been adequately rebutted, and a notice of allowance or a specific prior art showing of such claim features, in combination with the remaining claim elements is respectfully requested. (See MPEP 2112)

Issue # 3:

The Examiner has rejected Claims 3-6, 13, 16-19, 26, 29-32, and 39 under 35 U.S.C. 103(a) as being unpatentable over Chess in view of Smithson in view of Templeton (U.S. Patent No. 6,401,210).

Group #1: Claims 3-6, 13, 16-19, 26, 29-32, and 39

Appellant respectfully asserts that such claims are not met by the prior art for at least the reasons argued with respect to Issue #2, Group #1.

In the Examiner's Answer mailed 11/13/2006, the Examiner asserts that "Applicant's arguments… fail to comply with 37 CFR 1.111(b) because they amount to a general allegation that the claims define a patentable invention without specifically pointing out how the language of the claims patentably distinguishes them from the references." Appellant disagrees and respectfully points out that the arguments made hereinabove with respect to the independent claims in Issue #2, Group #1 sufficiently demonstrate that appellant's claim language is not met by the references cited by the Examiner. Thus, any claims depending therefrom are deemed allowable by virtue of their dependency on such independent claims.

Again, appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above.

In view of the remarks set forth hereinabove, all of the independent claims are deemed allowable, along with any claims depending therefrom.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 971-2573. For payment of any additional fees due in connection with the filing of this paper, the Commissioner is authorized to charge such fees to Deposit Account No. 50-1351 (Order No. NAI1P484).

Respectfully submitted,

By: ___/KEVINZILKA/_____   Date: _____January 15, 2007_____

Kevin J. Zilka

Reg. No. 41,429

Zilka-Kotab, P.C.
P.O. Box 721120
San Jose, California 95172-1120
Telephone: (408) 971-2573
Facsimile: (408) 971-4660